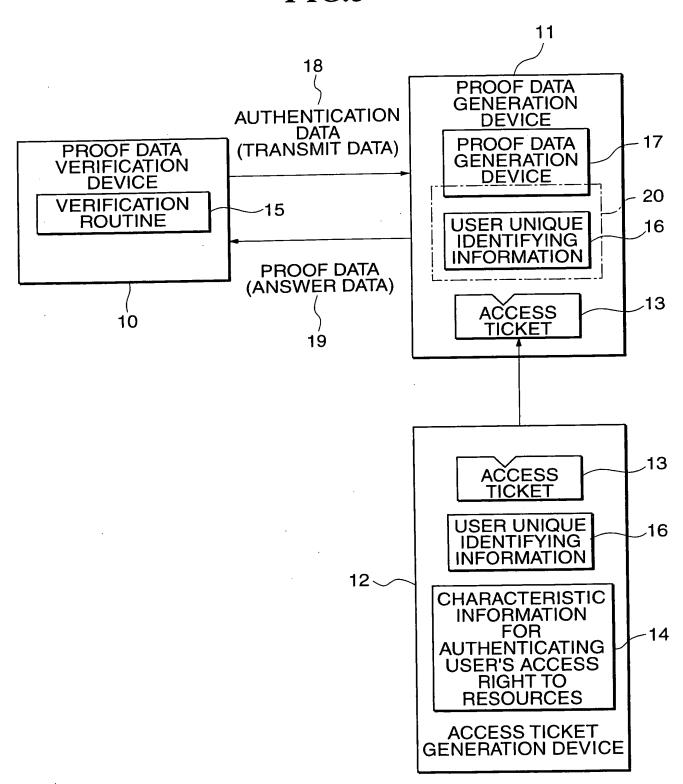
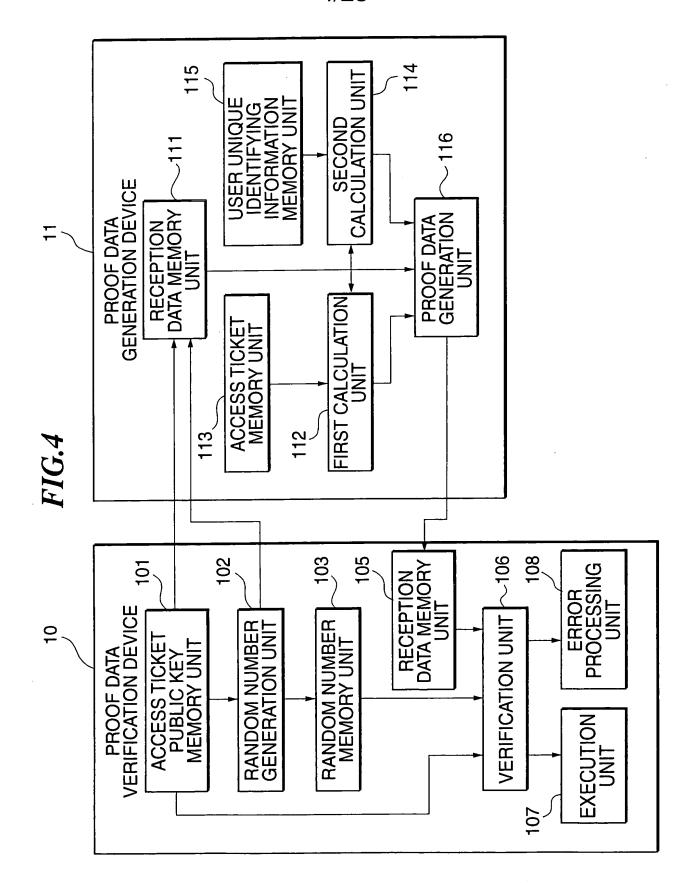
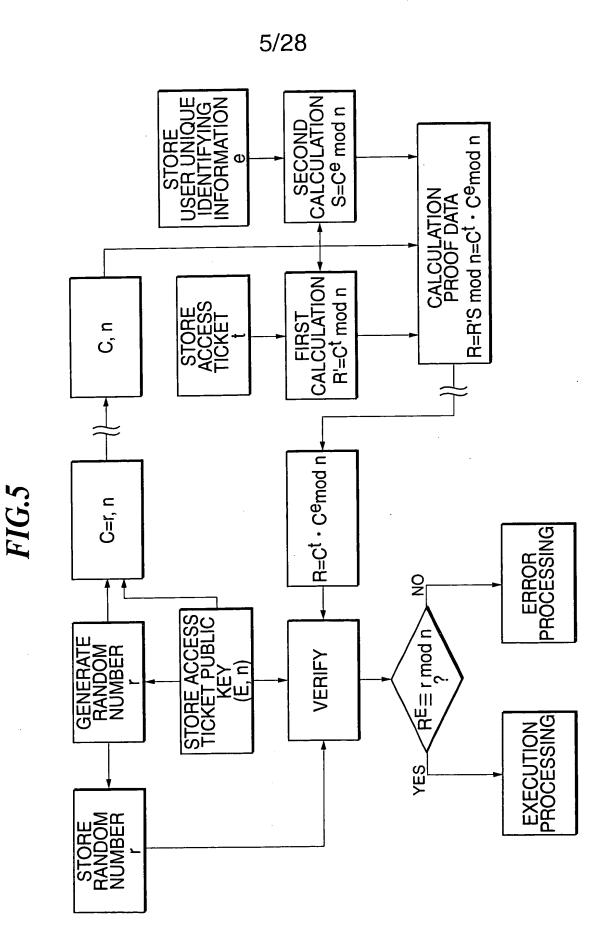


FIG.3







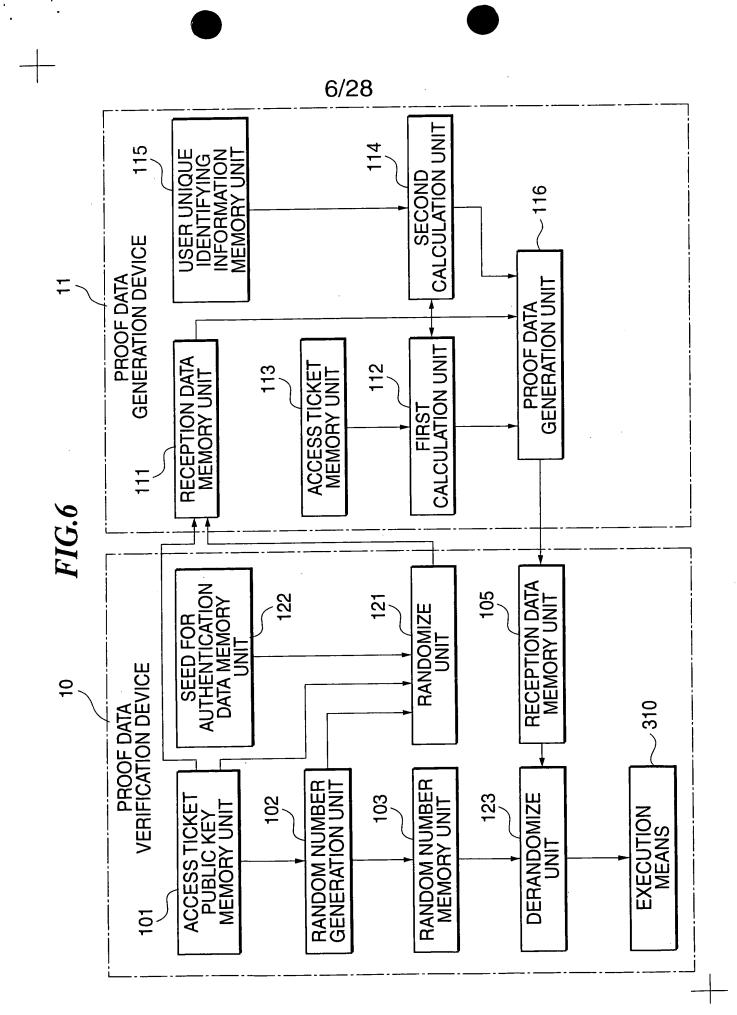


FIG.7

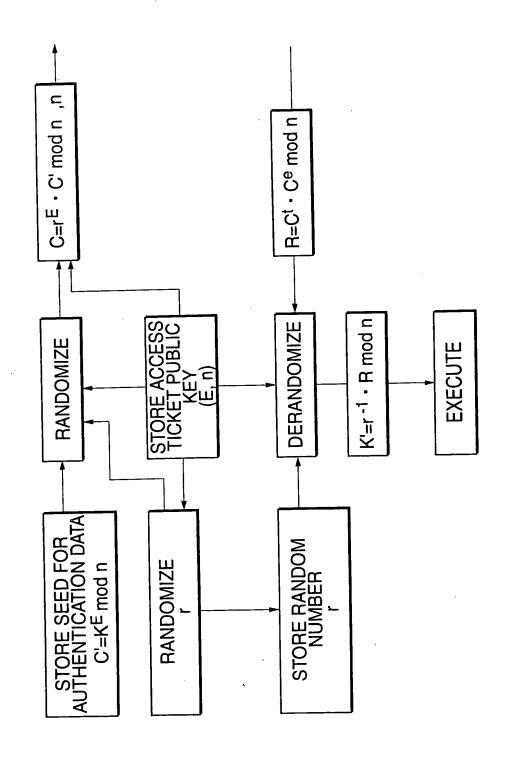


FIG.8

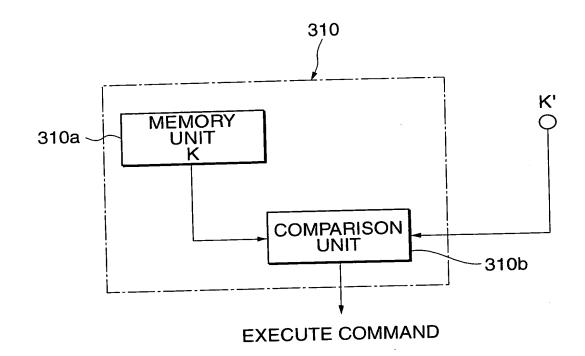


FIG.9

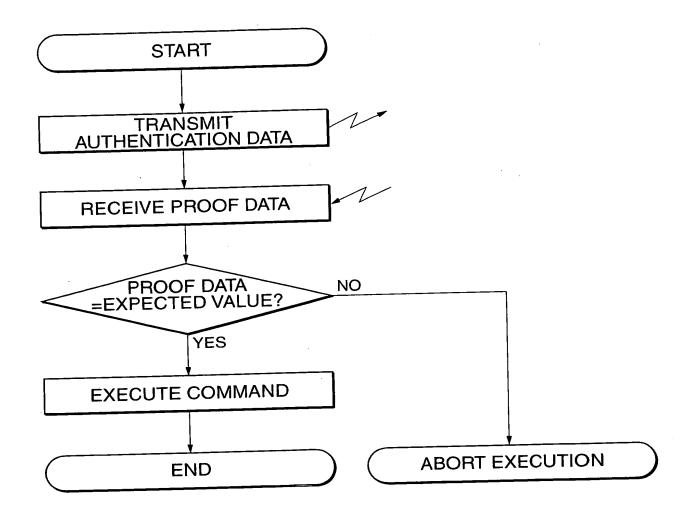


FIG.10

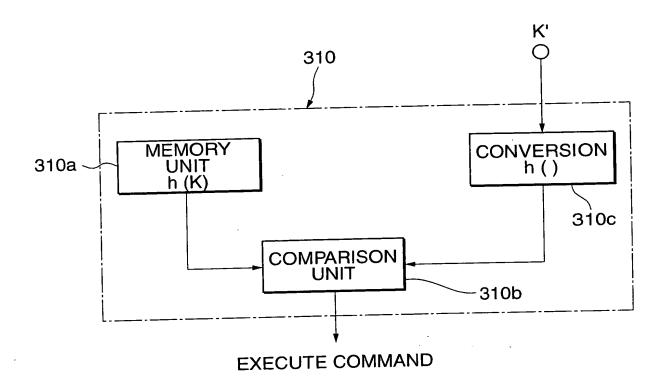


FIG.11

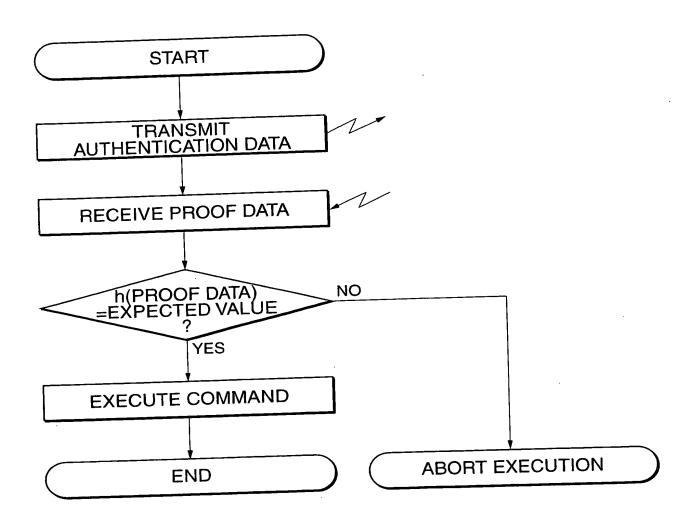


FIG.12

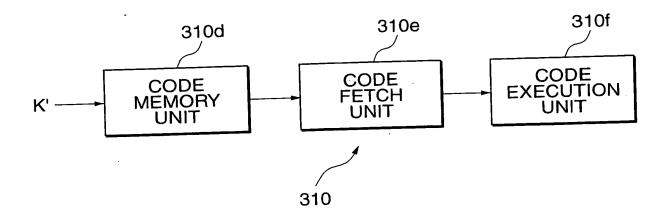


FIG.13

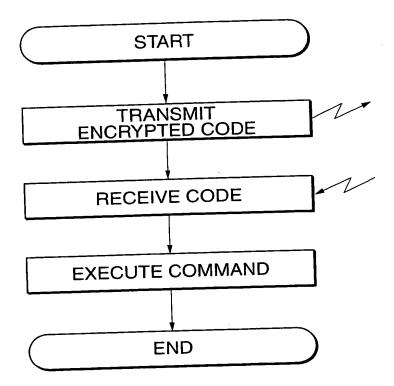
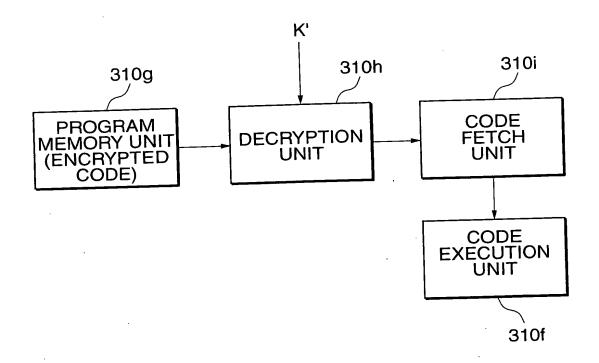
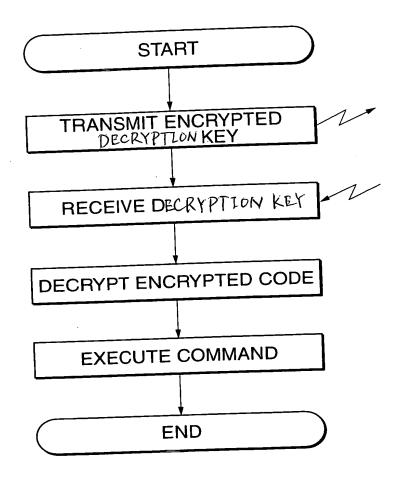


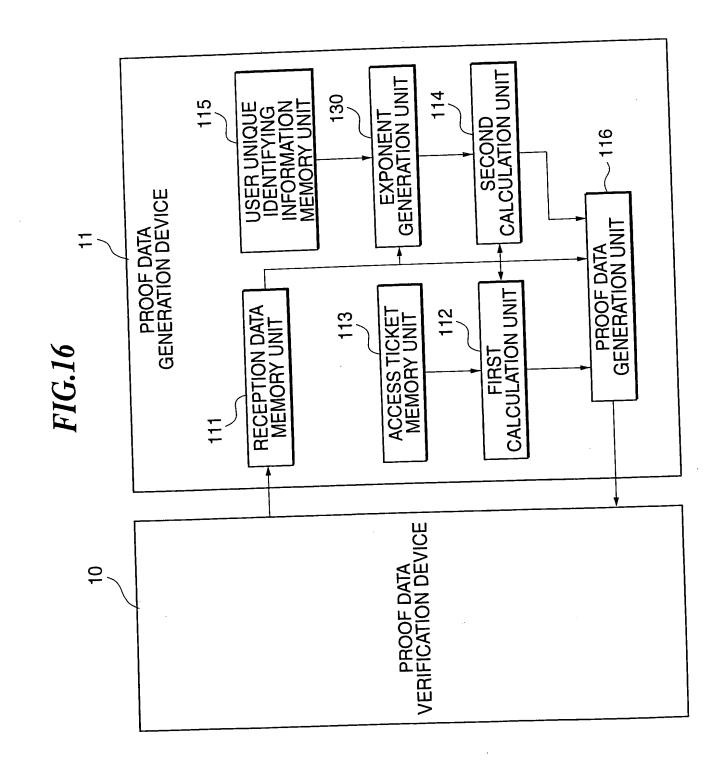
FIG.14



+-

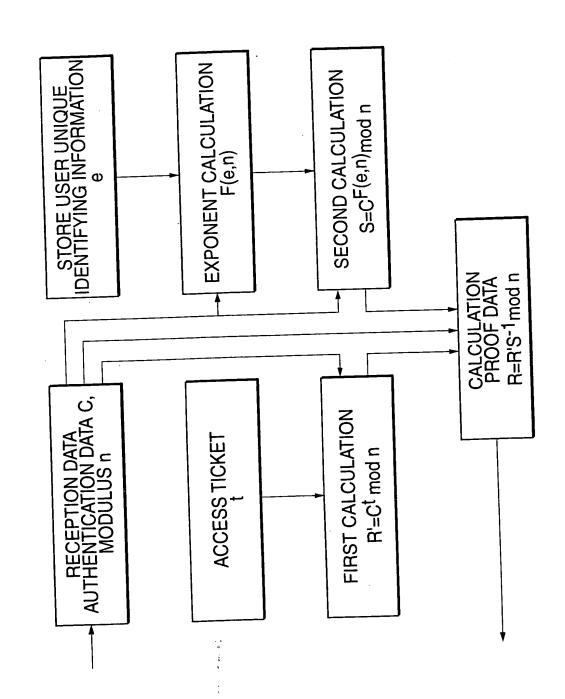
FIG.15

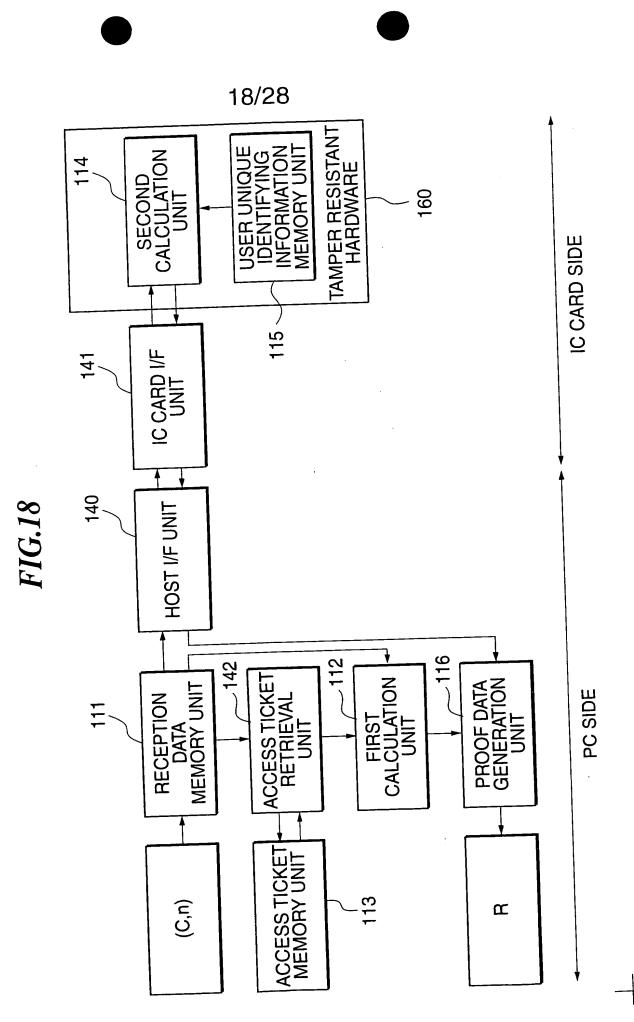


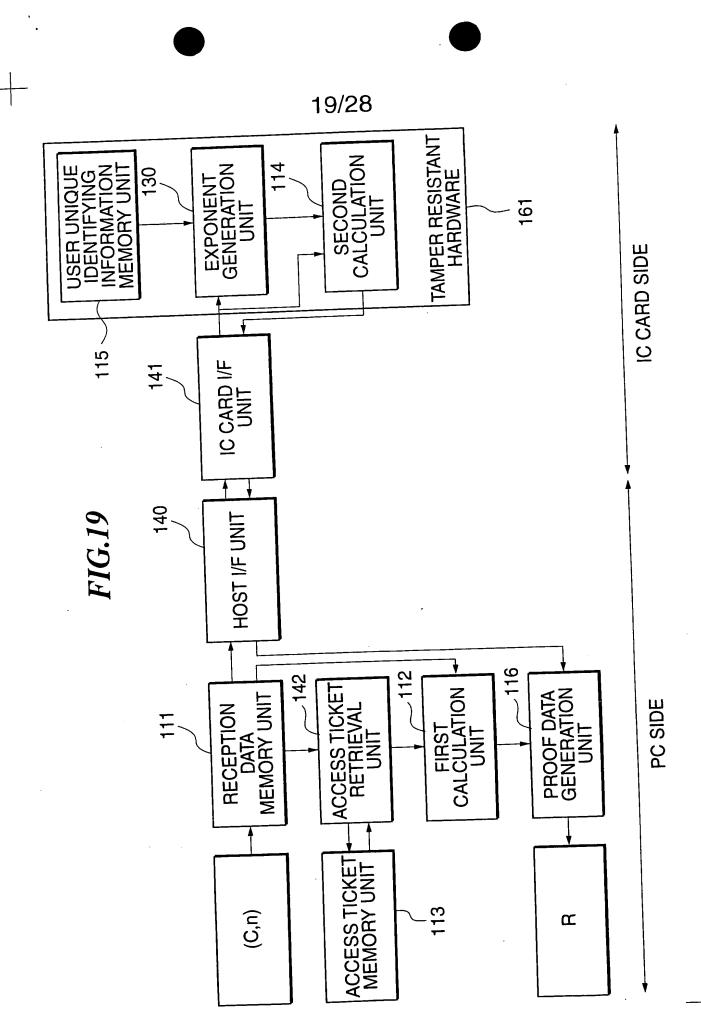


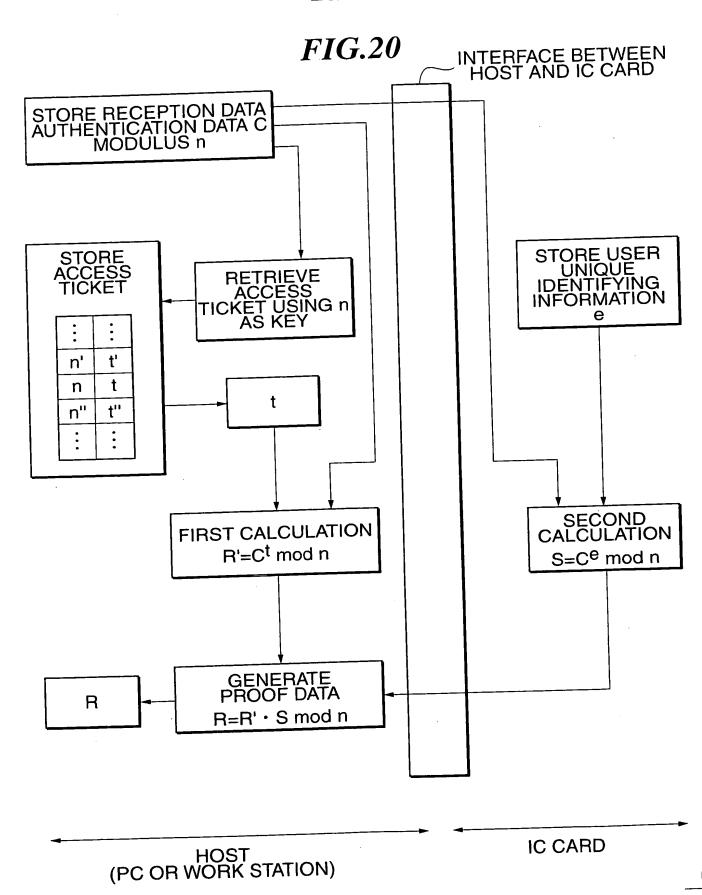
.

FIG. 17









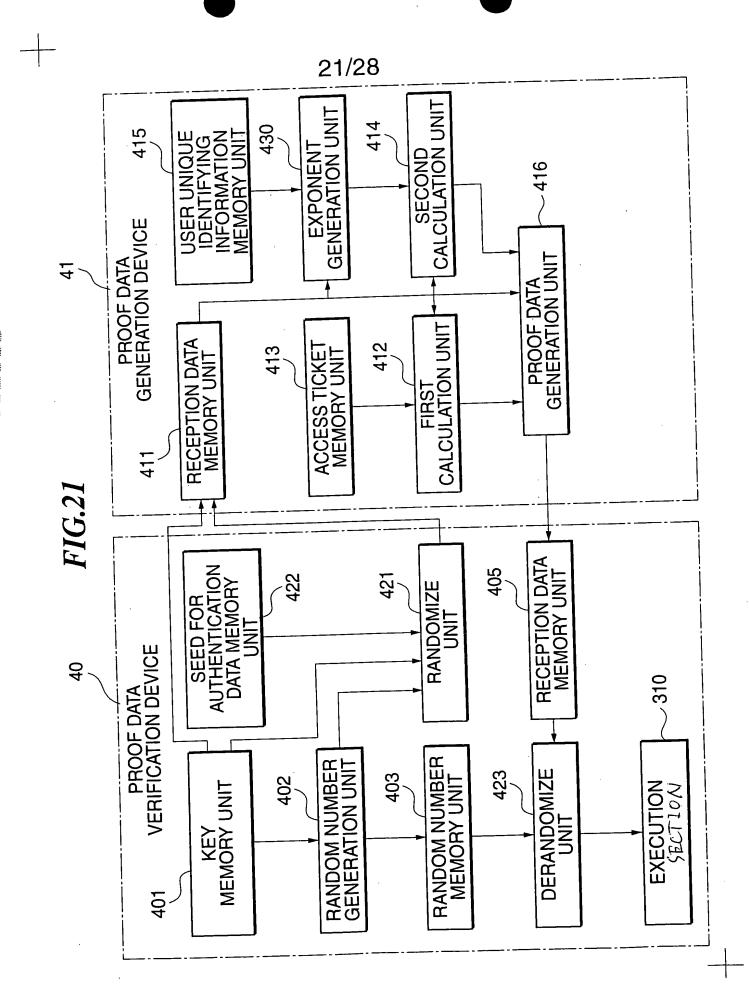
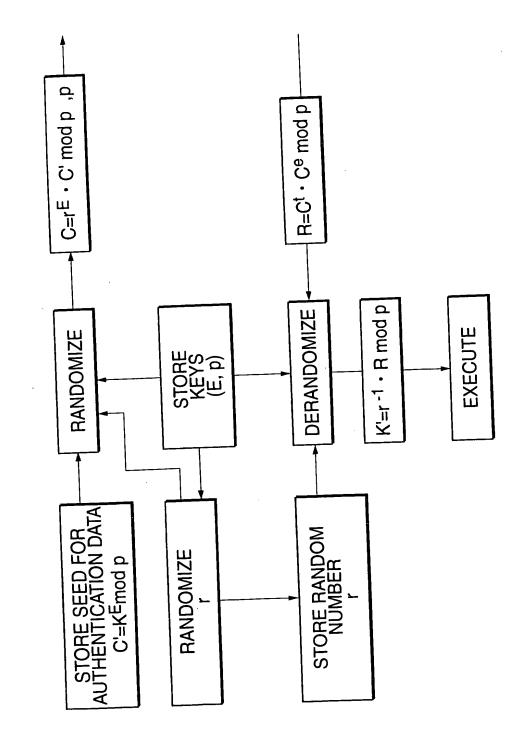
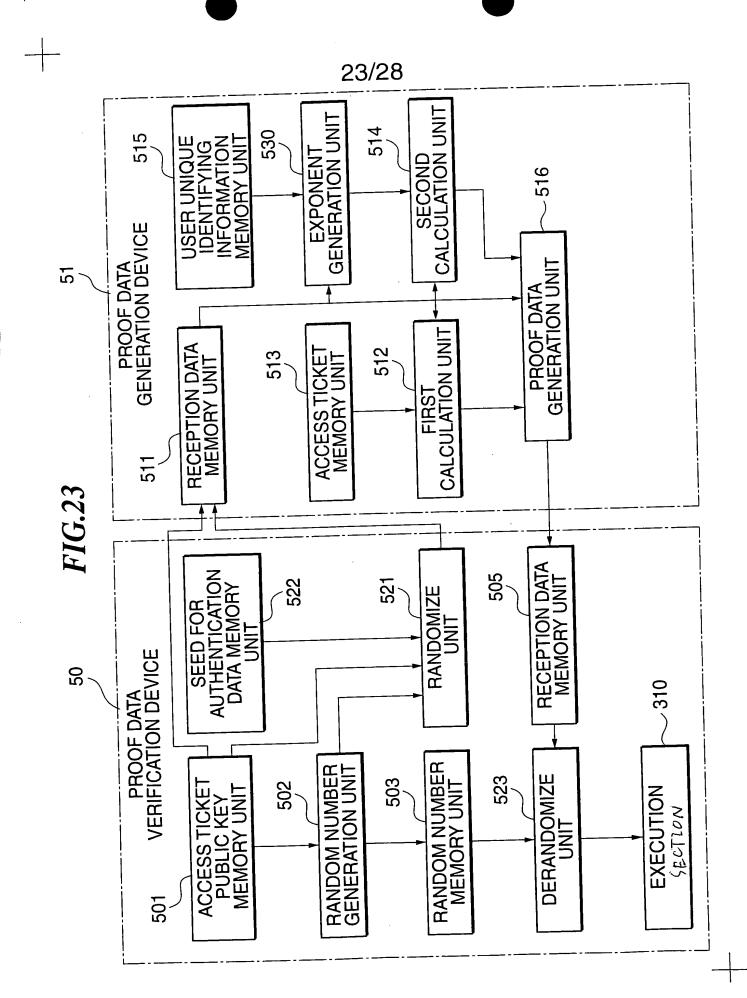


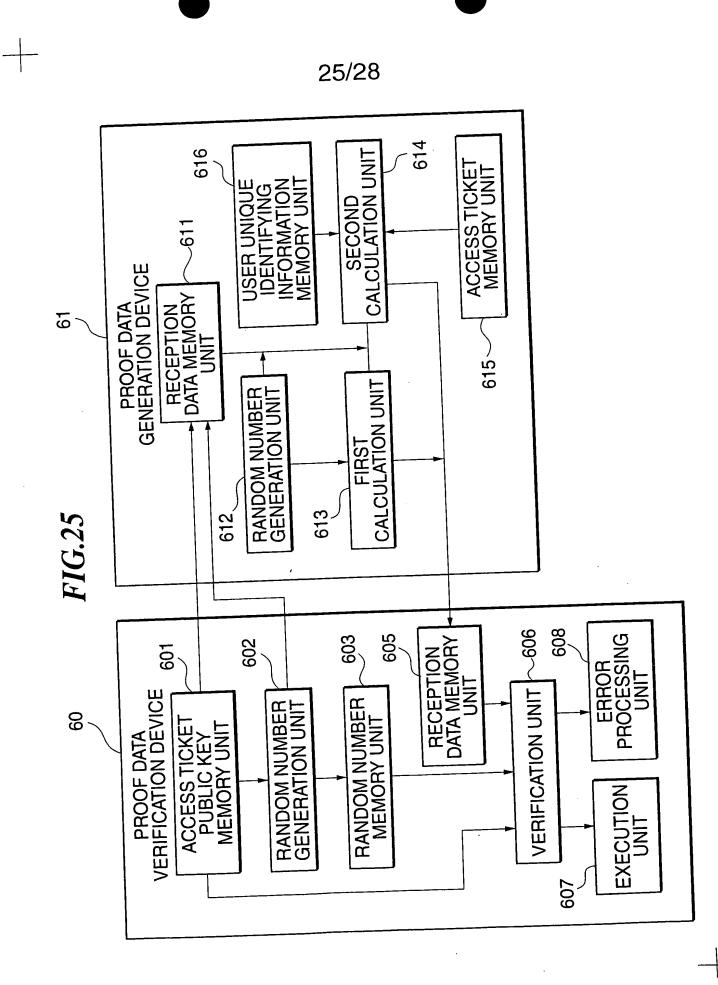
FIG.22

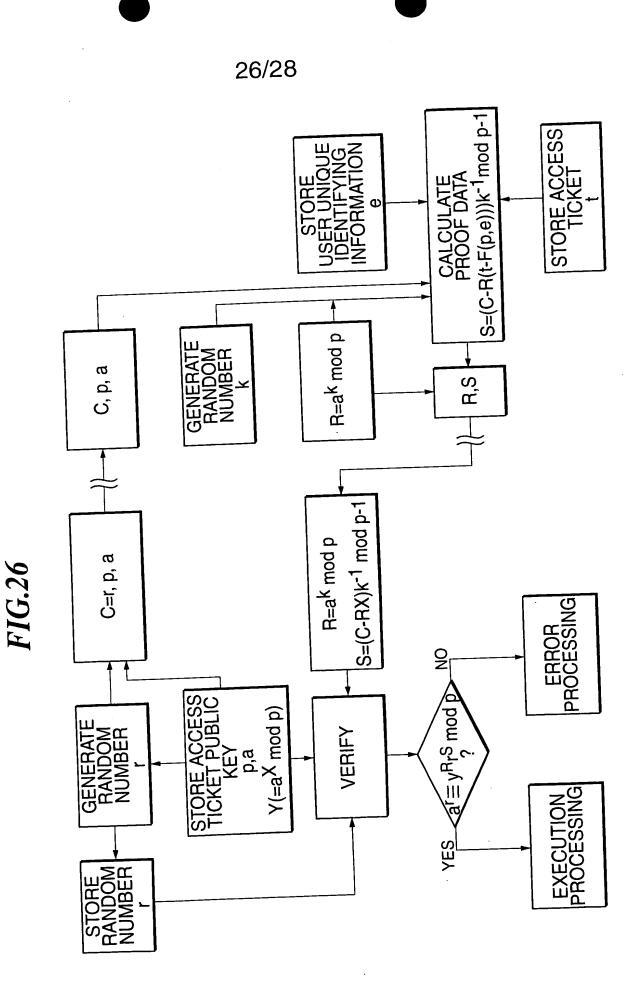




SECOND CALCULATION S'=u^F(p,e)mod p USER UNIQUE IDENTIFYING INFORMATION GENERATE EXPONENT CALCULATION PROOF DATA R=S⁻¹ · S' · mod p =u⁻¹ · u^F(p,e) · C mod p F(p,e) FIRST S=ut mod p STORE ACCESS TICKET p,u,C R=u-t · yF(p,e) · Cmod p $(=r \cdot u^{-X} \cdot \gamma^{Z} \cdot K \mod p)$ p,u C=rC' mod p STORE ACCESS TICKET PUBLIC KEY DERANDOMIZE K'=r-1R mod p $Y(=a^{X} \mod p)$ RANDOMIZE EXECUTE AUTHENTICATION DATA MEMORY UNIT u=a^z mod p C'=Y^zK mod p GENERATE RANDOM NUMBER STORE RANDOM NUMBER SEED FOR

FIG.24







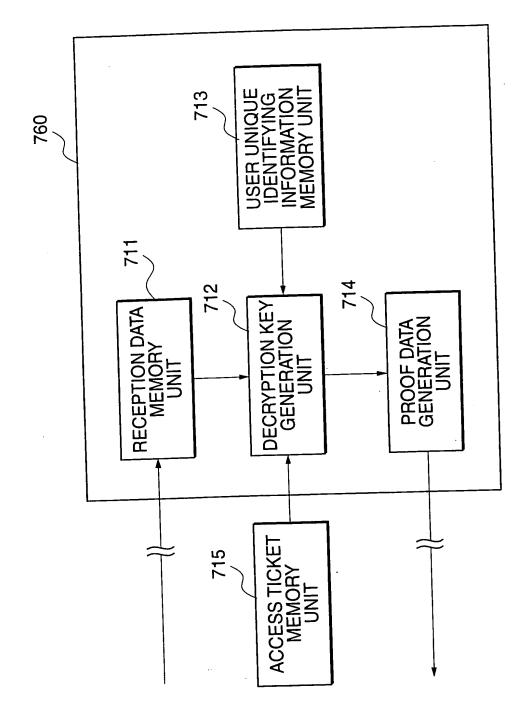
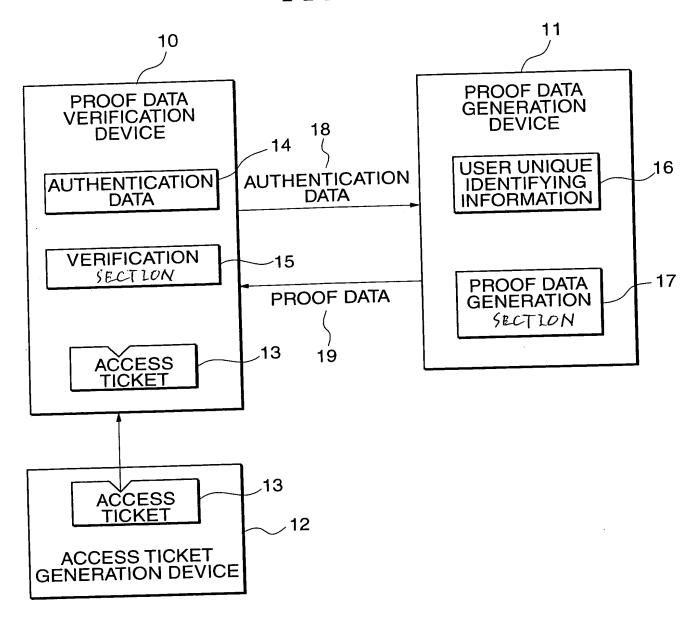


FIG.28



+-